CLAIMS

1. A method of securing packet data transferred between a first and second member of a private network over a backbone, the backbone operating according to a routing protocol, the method comprising the steps of:

receiving a packet;

apportioning the packet into a first portion and a second portion, wherein the first portion includes fields of the packet used for transmission of the packet according the protocol of the backbone;

transforming the second portion of the packet according to a group security association associated with the private network to provide a transformed portion;

appending the first portion of the packet to the transformed portion to provide a transformed packet; and

transmitting the transformed packet to the backbone using the private network address.

2. The method of claim 1, wherein the backbone comprises a plurality of provider devices, and wherein the step of transforming is performed by one of the plurality of provider devices in the backbone.

3. The method of claim 1, wherein an edge device is disposed between the first member of the private network and the backbone, and wherein the step of transforming is performed at the edge device.

4. The method of claim 1 wherein the step of transforming is performed at the first member of the private network.

5. The method according to claim 1, wherein the step of transforming the second portion of the packet comprises the steps of:

generating a group header associated with the private network;

appending the group header to the second portion of the packet prior to the step of transforming the second portion of the packet to provide a modified packet; and

transforming the modified packet according to the group security association associated with the private network to provide the transformed packet.

6. The method according to claim 5, wherein the first portion of the packet comprises a first header, the first header having a type, source and destination, and wherein the group header comprise a group type, group source and group destination, and wherein the step of generating a group header includes the step of copying the type of the first header to the group type.

7. The method according to step 6, wherein the first header further includes a length, the group header further includes a group length, and wherein the method includes the steps of copying the length to the group length.

8. The method according to claim 1 wherein the group security association is an Internet Protocol Security transform.

9. The method according to claim 8, wherein the group security association is an Encapsulated Security Protocol.

10. The method according to claim 1, wherein the group security association is an Internet Key Encryption.

11. The method according to claim 1, further comprising the step of receiving, at each member of the private network, a key corresponding to the private network group security association.

12. A method for securing a communication link between at least two members of a private network, the communication link for transporting a packet having first header and a payload, the

first header identifying a source address and a destination address packet, the method including the steps of:

distributing a security association to each of the at least two members of the private network;

transforming each packet transferred between the at least two members of the private network, the step of transforming including the steps of:

generating a second header, the second header including a source address associated with the source address in the first header, and a destination address identifying the private network;

replacing the first header of the packet with the generated second header to provide a modified packet;

applying the security association to the modified packet to provide a secure packet; and

appending the first header to the secure packet to provide a transformed packet; and

forwarding the transformed packet over the communication link using the private network address.

13. The method of claim 12, wherein the communication link comprises a plurality of provider edge devices, and wherein the step of transforming is performed at one of the plurality of provider edge devices.

14. The method of claim 12, wherein the step of transforming is performed at the one of the at least two members of the virtual private network.

15. The method of claim 12, wherein the step of transforming is performed at a gateway device disposed between one of the at least two members of the virtual private network and the communication link.

16. A method of receiving a packet transmitted between a first and second member of a private network over a backbone operating according to a protocol comprising the steps of:

receiving a packet from the first member of the private network for the second member of the private network, the packet including an address of the private network;

determining, responsive to the address, whether the packet received over the backbone is a secure packet;

responsive to a determination that the packet is a secure packet, stripping a first header from the packet to provide a remainder packet, the remainder packet comprising a group header and an encapsulated payload, and applying a group security association associated with the private network to the remainder packet, the remainder packet comprising an updated group header including fields associated with the protocol of the backbone.

17. The method according to claim 16, wherein the backbone comprises a plurality of provider devices, and wherein the steps of receiving, determining and stripping occur at one of the provider edge devices.

18. The method according to claim 16, wherein an edge device is disposed between the backbone and the second member of the private network, and wherein the steps of receiving, determining and stripping occur at the edge device.

19. The method according to claim 16, wherein the step of determining further comprises the step of analyzing bits of the packet that identify a type of the packet.

20. The method according to claim 16, wherein the first header and the group header each include a type field, and wherein the step of determining determines whether the type field of the first header and the type field of the second header correspond to predetermined values.

21. The method according to claim 16, further comprising the step of copying a type field from the updated group header into a type field of the first header, stripping the updated group header from the payload, and appending the first header to the payload to provide a restored packet for forwarding.

22. The method according to claim 16 further comprising the step of determining whether the group security association can be processed at the receiver.

23. An apparatus at a node for transforming packets for forwarding between a plurality of members of a group communicating on a scalable private network over a backbone, wherein the backbone operates according to a protocol, the apparatus comprising:

a key table, the key table including a security association for each group that the node is a member;

transform logic operable to apply a security association to only a portion of each packet transmitted over the private network associated with each group to ensure that a remaining portion of the packet enabling communication over the backbone according to the protocol is preserved; and

forwarding logic for forwarding communication between members of the group using an private network address associated with the group.

24. The apparatus of claim 23, wherein the backbone comprises a plurality of provider devices, and wherein the node is one of the plurality of provider devices.

25. The apparatus of claim 23, wherein at least one edge device is disposed between one of the plurality of members of the scalable private network and the backbone, and wherein the node is the at least one edge device.

26. The apparatus of claim 23, wherein the node is one of the plurality of members of the scalable private network.

27. An apparatus at a node for restoring transformed packets forwarded between a plurality of members of a scalable private network over a backbone, wherein the backbone operates according to a protocol, the apparatus comprising:

a control path including:

means for determining whether the packet is a transformed packet;

a key table, the key table including a security association for each private network that the node is a member;

restore logic operable to apply a security association to only a portion of each transformed packet, responsive to the means for determining indicating that the packet is a transformed packet.

28. The apparatus of claim 27 further comprising a forwarding path, wherein packets are always forwarded first to the control path to determine whether the packet is a transformed packet.

29. The apparatus of claim 27 wherein the backbone comprises a plurality of provider devices, and wherein the node is one of the plurality of provider devices in the backbone.

30. The apparatus of claim 27 wherein the node is an edge device disposed between the backbone and a receiving member of the scalable private network.